front page of WO97/28649 which corresponds to JPA 2000-504169

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION International Bureau [submitted in 09/832,981]

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 7/167 — A1

(11) International Publication Number: **WO 97/28649**

(43) International Publication Date: 7 August 1997 (07.08.97)

(21) International Application Number: PCT/FI97/00045

(22) International Filing Date: 29 January 1997 (29.01.97)

(30) Priority Data:
960418 30 January 1996 (30.01.96) FI

(71) Applicant *(for all designated States except US)*: OY NOKIA AB [FI/FI]; Eteläesplanadi 12, FIN-00130 Helsinki (FI).

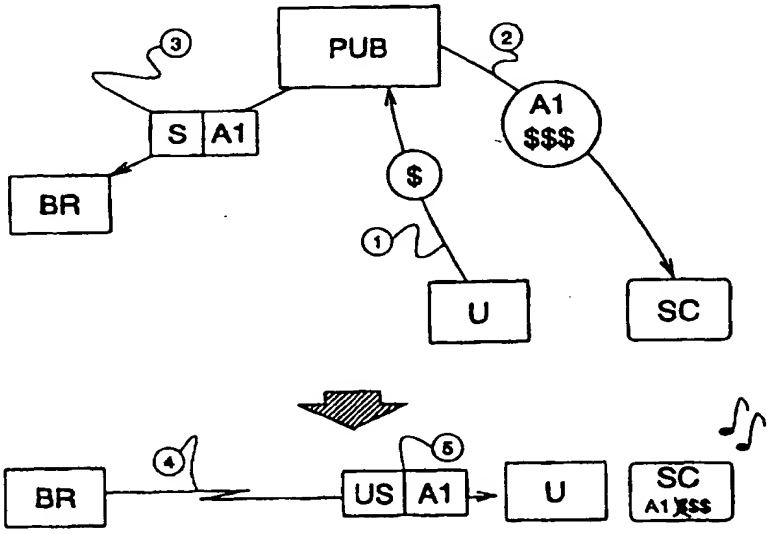
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: SALOMÄKI, Ari [FI/FI]; Auertie 7 C 42, FIN-04400 Järvenpää (FI).

(74) Agent: BERGGREN OY AB; P.O. Box 16, FIN-00101 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SCRAMBLING OF DIGITAL MEDIA OBJECTS IN CONNECTION WITH TRANSMISSION AND STORAGE



(57) Abstract

To prevent unauthorized reception, storage, copying and reproduction of digital media objects, it is defined in addition to a scrambled broadcast format a scrambled storage format which is different from the broadcast format. A user's terminal equipment cannot receive, store or reproduce protected objects without a key which is advantageously a bit sequence stored on a portable memory medium and which can be different according to the type of use it gives entitlement to. To prevent the storing and later reproduction as such of data in the broadcast format, a time stamp is included in the broadcast format representing the time of broadcasting. A playback device cannot reproduce a broadcast-format object if the reproduction time differs from the time stamp included in the broadcast format. The reproduction time is advantageously read from a real time clock of a portable memory medium.

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2000－504169
（P2000－504169A）
(43)公表日　平成12年４月４日(2000.4.4)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ

審査請求　未請求　予備審査請求　有　（全 31 頁）

(21)出願番号　特願平9－527329
(86)(22)出願日　平成９年１月29日(1997.1.29)
(85)翻訳文提出日　平成10年７月29日(1998.7.29)
(86)国際出願番号　ＰＣＴ／ＦＩ９７／００００５
(87)国際公開番号　ＷＯ９７／２８６４９
(87)国際公開日　平成９年８月７日(1997.8.7)
(31)優先権主張番号　９６０４１８
(32)優先日　平成８年１月30日(1996.1.30)
(33)優先権主張国　フィンランド（ＦＩ）

(71)出願人　オサケユイチア　ノキア　アクティエボラーグ
フィンランド国，02150　エスポー，ケイララーデンティエ　４
(72)発明者　サロマキ，アリ
フィンランド国，エフイーエン―04400　ヤルベンパー，アウエルティエ　７　セー　42
(74)代理人　弁理士　石田　敬　（外４名）

最終頁に続く

(54)【発明の名称】　伝送及び記憶に結びつけたデジタルメディアオブジェクトのスクランブリング

(57)【要約】
デジタルメディアオブジェクトの無許可の受信、記憶、コピー及び復元を防ぐため、スクランブルされた一斉通信書式に加えて、一斉通信書式とは異なるスクランブルされた記憶書式が定義づけされる。有利にはポータブルメモリ媒体上に記憶されたビットシーケンスでありそれが資格を与える用途タイプに応じて異なるものでありうるキー無くしては、ユーザの端末機器は、保護されたオブジェクトを受信、記憶又は復元することができない。一斉通信書式内のデータをそのままの状態で記憶し後日復元するのを防ぐため、一斉通信の時刻を表わすタイムスタンプが一斉通信書式の中に含まれている。復元時刻が一斉通信書式内に含まれるタイムスタンプと異なる場合、再生装置は、一斉通信書式のオブジェクトを復元できない。復元時刻は、有利には、ポータブルメモリ媒体の実時間クロックから読み取られる。

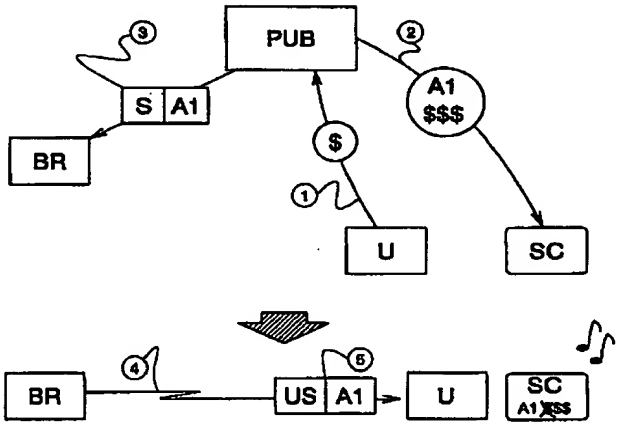


Fig. 2

【特許請求の範囲】

1．無許可の使用に対しデジタルメディアオブジェクトを保護する方法であって、前記オブジェクトは複数の受信者に対し電気的に配給可能でありかつ後日の使用のためにメモリ媒体上に記憶可能であり、前記メディアオブジェクトのためにスクランブルされた一斉通信書式が定義づけされているような方法において、メモリ媒体上への前記記憶のための前記メディアオブジェクトのためにスクランブルされた記憶書式もまた定義づけされ、このスクランブルされた記憶書式は前記スクランブルされた一斉通信書式と異なっていることを特徴とする方法。

2．前記スクランブルされた記憶書式の中で、メディアオブジェクトは、予め定められた構造をもち記憶されるべき実際のデータ及びその記憶に関連するその他の情報を含むフレームの形に分割されることを特徴とする請求項１に記載の方法。

3．前記スクランブルされた一斉通信書式と区別するため、各フレーム内の前記その他の情報には、その書式が記憶書式であることを告げる一片の情報が含まれていることを特徴とする請求項２に記載の方法。

4．各フレーム内の前記その他の情報のうちの少なくとも一部分は、秘密のアルゴリズムにより決定される要領で保護されるべき情報に基づいて内容が決定されるデータ部分を記憶書式内に内含することによって保護されていることを特徴とする請求項２又は３に記載の方法。

5．前記スクランブルされた一斉通信書式及びスクランブルされた記憶書式が、一斉通信書式の中では一斉通信の時刻を表わし、記憶書式の中では記憶時刻を表わすようなタイムスタンプを内含して

いることを特徴とする請求項１～４のいずれか１項に記載の方法。

6．メディアオブジェクトがユーザに復元された時点で、問題のオブジェクトが一斉通信書式であるか否かが検査され、そうであれば一斉通信書式に含まれているタイムスタンプが復元時刻と比較され、かくして一斉通信書式内のタイムスタンプと復元の時刻の間に予め定められた最大値よりも大きな差異がある場合、オブジェクトの復元が妨げられるようになっていることも要求されることを特徴

とする請求項５に記載の方法。

7. 特定のメディアオブジェクトを使用しかつ／又は記憶するための資格が、ポータブル式メモリ媒体上に記憶されたキーの形でユーザに送り出されることを特徴とする請求項１～６のいずれか１項に記載の方法。

8. 復元の時刻が、前記ポータブル式メモリ媒体内に含まれたクロックから読取られることを特徴とする請求項６又は７に記載の方法。

9. スクランブルされた一斉通信書式をスクランブル解除するための手段をそなえて成る、デジタルメディアオブジェクトをユーザに対し受信し記憶し復元するための端末機器において、前記スクランブルされた一斉通信書式とは異なるものであるスクランブルされた記憶書式の中に受信されたメディアオブジェクトを記憶するための手段もそなえて成ることを特徴とする端末機器。

10. メディアオブジェクトの復元と結びつけて一斉通信書式内に内含されたタイムスタンプを復号し、前記タイムスタンプを復元の時刻と比較するための手段をそなえて成ることを特徴とする請求項９に記載の端末機器。

11. ポータブル式メモリ媒体から復元の時刻を読取るための手段をそなえて成ることを特徴とする請求項10に記載の端末機器。

【発明の詳細な説明】

伝送及び記憶に結びつけたデジタルメディアオブジェクトのスクランブリング

本発明は一般に、無許可の受信及びコピーに対するデジタルサウンド及びピクチャーオブジェクトの保護に関し、特に、一斉通信（broadcasting）、局所記憶(local storage)及び消費者に対する録音録画物（recordings）の販売及び配給に関し均等なやり方でいかに無許可受信及びコピーに対する保護を実施できるか、に関する。

画像及び／又はサウンドを含むプログラム及びプレゼンテーションの電気的伝送及び記憶は、アナログからデジタル技術へと移行し、現在も移行し続けている。デジタル技術のもつ利点は、スプリアス効果に対する感受性が低いこと、及び汎用性ある誤り補正の可能性にある。デジタル画像及びサウンドの品質は、アナログ技術を使用していた時と同じ形で伝送、受信及び記憶した際に劣化することがない。デジタル技術はすでに、コンパクトディスク、つまりCDの形でのオーディオ及びデータ録音録画物の販売及び配給において広く使用されている。コンピュータが、大量記憶装置内へのデータのデジタル磁気記憶を応用し、デジタル一斉通信システムが試験段階にある。我々は、将来において、データ伝送及び記憶の容量及び開発利用の両方が増大し続けるものと想定することができる。

以下では、１つのエンティティとして取り扱われる全てのデジタルサウンド及び画像の録音録画物及び伝送を、単純にオブジェクトと呼ぶことにする。オブジェクトとは、ピクチャ、音響効果、楽曲、映画、アニメ番組、ラジオ番組、マルチメディアプログラム又は、そのままの状態で及び／又は他の対応するオブジェクトと合わせ

てユーザに対し伝送、記憶及び復元する(reproduce)ことのできるその他の対応するエンティティであり得る。伝送というのは、特に、伝送局が定期的に多数の受信者に対し電気的にオブジェクトを配給する一斉通信のことを意味する。記憶というのは、オブジェクト又はそこから抽出された周期が、後に復号されて必要な場合には何度もユーザに復元され得ることになるような１つの形態にされることを意味する。

コンピュータプログラムは、同じ形で一斉通信されるものではないものの、やはり一種のオブジェクトとみなすことができる。マルチメディア及び対話型マスメディアがさらに民間に普及していくにつれて、我々の知っているコンピュータプログラムと（娯楽的なものであれ教育的なものであれ）ラジオ又はTV番組の間の境界はあいまいになってくる。例えば、デジタルオーディオ一斉通信(DAB)システムは、ファイル書式で一斉通信され、ユーザにプログラムの流れを変える可能性を与えることになるようにユーザに対し後に対話式に復元されるべき受信機器の記憶媒体の中にロードされるオブジェクトを伝送する。

デジタル録音録画物は容易に復元され得ることから、版権所有者からの許可の無い受信及び復元ができるかぎりむずかしいものとなるように、伝送及び記憶と結びつけてオブジェクトを暗号化又はスクランブルする必要性が発生した。この措置の目的は、１つのオブジェクトの製作者及び／又は配給業者が受信者及び／又はユーザから或る一定の報酬を得るということにある。ユーザが、使用目的でオブジェクトをスクランブル解除（デスクランブル）できる復号装置又はキーを取得するというのが一般的である。料金の対象となるTVチャンネル上で送られたプログラムをスクランブル解除するいわゆるブラックボックスが、先行技術から知られている。スクランブ

ル解除装置は、例えばスクランブル解除に必要とされるコードワードを含むいわゆるスマートカードによって制御され得る。スクランブルされた伝送がスマートカード内に記憶されたキーを用いてスクランブル解除される類似の方法が、例えば、GSM 移動電話システムでのデジタルデータ伝送において応用されてきた。

先行技術によるスクランブリング及びスクランブル解除の方法及び装置は通常、それらがチャンネル特定的であることを特徴としている。すなわち、スクランブリングは伝送ストリームがどんなオブジェクトを含んでいるかに関わらずつねに同じやり方で特定の伝送ストリームに向けられているのである。唯一のオプションは、例えば有料TVチャンネルが、より多くの視聴者が見れるようにスクランブルされていない特定の映画又は番組を送信したい場合のスクランブリングのオンオフ切換えである。しかしながら、版権はつねに個々のオブジェクトに向けら

れており、従って、先行技術による方法は、異なる供給源から取得したオブジェクトの製作者が、伝送局が自らの配給網又は受信可能範囲（カバレージエリア）内で特定のオブジェクトを一斉通信する権利について支払いを行なう場合以外の何らかの方法で報酬を受けることができるような有料システムを実現することができない。

先行技術による方式はまた、スクランブリング解除装置を意のままにできる受信者が制限無く特定のオブジェクトをスクランブル解除後に記憶し復元しさらに配給できるということを特徴としている。オブジェクトを製作する当事者及びその伝送及び配給サービスの権利を保護するためには、１つのオブジェクトを記憶し復元することに対する別途の報酬を支払うようユーザに義務づけることが非常に大切である。

コンピュータソフトウェアに関しては、プログラムを使用可能に

するためにコンピュータの通信ポート内に挿入されなくてはならないプラスチックハウジング内に成形された電気回路を通常含む、固定キー装置又はいわゆるハードロックが使用される。この方式を用いると、通常のユーザはハードロックを復元できず、復元されたプログラムコピーはハードロック無しでは機能しないことから、或る程度までオブジェクトの復元を防止することが可能である。しかしながら、ハードロックが特定のオブジェクトの特定のバージョンに結びつけられ、オブジェクトが一斉通信タイプの伝送においてそうであるように常時変動し変化する場合にはより広いベースで応用できないことから、この方式はむしろ融通性がない。

本発明の目的は、オブジェクトの伝送、受信、記憶及び復元を網羅する、電気的に伝送されたオブジェクトをスクランブルしまたスクランブル解除（デスクランブル）するための方法を提供することにある。本発明のもう１つの目的は、前記スクランブリングに対し、オブジェクトを製作する当事者及びオブジェクトのための伝送及び配給サービスにスクランブル解除権に対応する報酬を導く支払いシステムを付加する方法を提供することにある。本発明のさらにもう１つの目的は、そのようにした方法を既知のデジタル伝送及び記憶方式に応用できるように

することにある。

本発明の目的は、記憶及び一斉通信のために異なるスクランブリングデータ書式（フォーマット）を用いて、デジタルデータの一斉通信及び記憶において応用されるべき一般的な標準化されたスクランブリングデータ書式を定義することにより達成される。本発明の目的の達成は、ユーザのスクランブル解除装置に実時間クロックを付加すること、実時間コードをデジタル一斉通信書式に組合わせること、そしてスクランブル解除権に対応する支払い取引をスクランブル解除キーの配給と組合わせることによってさらに促進すること

ができる。

複数の受信者に電気的に配給され、後日使用するためにメモリ媒体上に記憶することのできるデジタルメディアオブジェクトを無許可の使用に対し保護するための本発明による方法は、スクランブルされた一斉通信書式が前記メディアオブジェクトについて特定されているような方法であり、このスクランブルされた一斉通信書式とは異なるスクランブルされた記憶書式もまた、前記メモリ媒体上での記憶のため前記メディアオブジェクトについて特定されることを特徴としている。

本発明はまた、スクランブルされた一斉通信書式をスクランブル解除するための手段を含む、ユーザに対するデジタルメディアオブジェクトを受信し記憶し復元するための端末機器にも関する。本発明による端末機器は、前記スクランブルされた一斉通信書式とは異なるスクランブルされた記憶書式内に、受信したメディアオブジェクトを記憶するための手段をさらに含むことを特徴としている。

本発明は、共通の国際協定又は規格がデジタルメディアオブジェクトについて、それらが伝送中であるか記憶中であるかに応じて異なるスクランブルされた書式又は識別手順を定義づけできる、ということを意味している。さらに、１つのオブジェクトについて、それが（版権所有者によって製作された）オリジナル版であるかその他の誰かによって製作されたコピーであるかによって、異なる書式又は識別手順を特定することができる。問題のオブジェクトの復元を許可するキーを自由に使える場合にのみ受信又は記憶されたオブジェクトを復元できるよう

な形で、デジタルメディアオブジェクトを取扱う装置が製造される。その上、本発明の有利な実施形態においては、該装置は一斉通信書式のオブジェクトを記憶せず、まずそれらを記憶書式に変換することになる。オブジェクトは、一定サイズのデータ部分つまりフレームとして有利に取扱われ、かくして、一斉通信書式と記憶書式の間の差は、フレームヘッダ部分又はパケットの内容を記述するその他のデータ構造の中で１ビット又はビット組合せの変化程度に小さいものであり得る。

本発明によるスクランブリング方法は、さらに、伝送されたオブジェクトがタイムスタンプを受ける、つまり伝送の瞬間を表わすデータが備えられているようなタイミング方式を含んで成る。このとき、一斉通信書式内に１つのオブジェクトが記憶されていたとしても、復元装置がまず最初に記憶された時刻データを実時間と比較しなければならないならば、後にそれが無許可で復元されることを防ぐことができる。時刻が同一でない場合には、復元は禁止される。このタイミング方式は、有利にはスマートカードのようなものである電気的メモリ媒体に基づいている。以下では、このポータブル式メモリ媒体をスマートカードと呼ぶことにする。本発明の好ましい実施形態による方式では、スマートカードは実時間クロックを含んでおり、これは、任意の時間的瞬間で読取られたとき、読取り時刻を表わすデータを無条件に生成するようなあらゆる回路全般を意味する。本発明によると、各オブジェクトは、伝送及び記憶の両方のために、フレーム、パケット、セル又はデータグループと呼ぶことができしかもデータ伝送及び／又は記憶について記述する既存の標準及び推奨事項に従って書式化されているデータ部分の形に整備される。フレーム及びデータグループの少なくとも一部分には、一斉通信の場合には伝送時刻を表わし記憶の場合には記憶時刻を表わすタイムスタンプが具備されている。

オリジナル録音録画物（例えばCD）として配給されるか又は伝送されるべきオブジェクトの内容は、有利には比較的大きい２進数字である或る種の暗号キーがスクランブル解除に必要とされる既知の

方法を用いてスクランブリングされる。ユーザは、自らが或る一定の金額を支払った時点で必要な単数又は複数のキーがそのスマートカード内にロードされることになるように、問題のオブジェクトを使用する権利を購入することができる。キーは確定された又は無期限の期間中有効でありうる。伝送されたオブジェクトの場合には、ユーザは、自らがオブジェクトを一回だけ使用するか（実時間使用）又は後で場合によっては数回使用するべくそれを記憶（コピー）するかに応じて、異なる金額を支払う。ここで「使用する」という語は、広義に、オブジェクトを検分する（見る）、聞く又はその他の形で開発利用することを意味している。実時間使用及び記憶のための価格が異なることから、スマートカード内に記憶されるキーは、異なる使用目的のために異なるものでなくてはならない。

本発明について、一例として示された好ましい実施形態ならびに添付図面を参照しながら、さらに詳細に記述する。なお図面中、

図１は、本発明による方法の適用における一形態を示す。

図２は、本発明による方法の適用におけるその他の形態を一連のピクチャとして示す。

図３は、本発明による方法の変形適用形態を示す。

図４は、本発明による方法のもう１つの変形適用形態を示す。

図面中の同じ要素は、同じ参照記号で表わされている。

本発明は、デジタルオブジェクトの一斉通信を提供することから、まず第１に、適用例としてここで用いられるデジタルオーディオ一斉通信（DAB)システムの基本的特長について記述することにする。DAB システムにおいては、オーディオ伝送内及びデータ伝送内での情報全般は、オーディオ伝送の場合にはオーディオフレームと呼ばれ、データ伝送の場合にはデータグループと呼ばれる一定サイズのデータ部分の形で搬送される。各々のオーディオフレーム及びデータグループは、その内容を記述するフィールド又は記録を含むヘッダ部分、及び伝送されるべき実際のデータを含むペイロード部分を内含する。さらに、DAB システムは、当業者にとっては既知のやり方で、送信装置から受信装置までフレーム特定的な及びさらに一般的な制御情報の両方を転送するのに用いられるデー

タ構造を規定している。このようなデータ構造の最も重要な形態は、いわゆる高速情報チャンネル（FIC)上で転送される高速情報グループ（FIG)及び、オーディオフレームの場合にはフレーム特定的プログラム関連データ（PAD)フィールドである。

DAB システムは、以下のオーディオフレーム特定的データ(audio frame specific data)及びスクランブリングされたオーディオ一斉通信を伴うその伝送を規定している：

１ａ）既知の又は暗号化されたキーを用いたフレームのスクランブリング

DAB システムにおいては、スクランブリングと暗号化は、異なるものを意味している。スクランブリングというのは、或る一定のキーを知らなければ中に含まれているサウンドを復元（再生）できなくなるようにオーディオデータを変更することである。このキーは、擬似乱数（pseudo-random number）を生成する或るジェネレータに対するシード（種）として供給されたとき、問題のキーに対応する擬似ランダムビットシーケンスを生成するような数である。ビットシーケンスとスクランブルされたオーディオデータの間で実行される論理XOR(排他的論理和）動作が、復元可能なオーディオデータを生成する。スクランブリングと反対のこのオペレーションはスクランブ解除（デスクランブリング）と呼ばれる。ユーザに与えられるキーは、クリア（既知）であっても暗号化されたものであってもよい。暗号化されている場合、暗号化されたキーはまず第１に解読

されなくてはならない。キーの暗号化を実施する方式はいくつか存在しており、これについては後で立ち戻ることにする。この段落では、DAB システム内のオーディオフレーム特定的データは、問題のフレームが既知のキーを用いてスクランブルされるか又は暗号化されたキーを用いてスクランブルされるかを示すという事実に言及しておく。

１ｂ）使用される条件付きアクセスシステム

より広い概念としての暗号化手順は、サービスのアクセス権に関係するいくつかの仕様を含む条件付きアクセスシステムの中に内含されている。既知の条件付きアクセスシステムの中には、なかんづく、ユアロクリプト（Eurocrypt)及びNR

-MSKが内含されている。適用される条件付きアクセスシステムは、各フレームについて示すことができる。

１ｃ）暗号化アルゴリズム

キー暗号化手順において適用される計算方法を識別（特定）する或る一定のアルゴリズムのためのコード。

１ｄ）タイムスタンプ

日付及び／又は時刻を表わすタイムスタンプを、それが伝送時刻に対応するような形で各フレーム内に内含させることができる。

１ｅ）許可データ（authorization data)

各フレームには、伝送されたオブジェクト、及び例えばそのオブジェクトを生成してそのオブジェクトの版権の所持者である当事者を識別（特定）する識別情報が内含されることができる。

１ｆ）暗号化されたキー

１ｇ）初期化修正子（initialization modifiers)

標準的に、スクランブリングキーは、数フレームのみについて有効である。さらにこれらのフレーム間でいわゆる初期化、すなわち

リセットも実行でき、長いビットシーケンス内で考えられる誤りが比較的無害となるようにスクランブル解除において用いられる擬似ランダムビットシーケンスジェネレータがリセットされる。初期化修正子は、ジェネレータがいかに初期化されるかを定義づける。

１ｈ）スクランブルされた伝送されるべきオーディオフレーム

さらに、DAB システムは、以下のデータグループ特定的情報及びスクランブルされたデータの伝送を伴うその伝送をも規定する：

２ａ）既知の又は暗号化されたキーでのフレームのスクランブリング

１aと同じ。

２ｂ）使用される条件つきアクセスシステム

１bと同じ。

２ｃ）暗号化アルゴリズム

１ｃと同じ。

２ｄ）タイムスタンプ

１ｄと同じ。

２ｅ）許可データ

１ｅと同じ。

２ｆ）暗号化されたキー

２ｇ）初期化修正子

１ｇと同じ。

２ｈ）伝送されるべきスクランブルされたデータグループ

さらに、DAB 勧告は、以下の情報に関するファイル特定的伝送を規定している：

２ｉ）ファイル名又はid番号

２ｊ）ファイル内のデータグループ（ブロック、セグメント）の数

２ｋ）各バイト内のファイルサイズ

２１）修正されたファイルについてのファイルバージョン数

次に、我々は、本発明によって、記憶されるべきオーディオフレームに付加されることになるフレーム特定的データを見て行くことにする。提示された記録の数、順序及びサイズならびにビット値及びビット組合せの定義は、一例として示されているにすぎず、発明を制限することを意図されたものではない。

３ａ）オーディオフレーム計数、24ビット

特定のオブジェクトに関係する記憶されたフレームは、連続的に番号づけされる。提案された24ビットの番号づけフィールドは、2^{24}のフレームを識別するために使用することができる。各々のフレームが、DAB 規格に従って24ミリセカンドのプレイバック周期に対応する場合、記憶されたオブジェクトの最大持続時間は約$4^{1}/_{2}$日である。フレームの連続的番号づけは、特に高速巻戻し、高速前送り及びサーチといったようなオペレーションにおいて有利である。

３ｂ）オリジナル／コピー、１ビット

１つのいわゆるフラグビットが、そのオブジェクトがオリジナル版であるかコ

ピーであるかを示す。例えば、フラグビット値１は、オリジナルを表わし、０はコピーを表わす。フレーム特定的フラグビットを０に設定するような形で、記憶（コピー）装置を構築しなくてはならない。

３ｃ）記憶属性、２ビット

２ビットを用いて、問題のオブジェクトについてどの種類の使用が許されるかを示すことが可能である。以下の表は、ビット組合せの有利な仕様を示している。

表１：スクランブルされたオーディオオブジェクト

ビットｂ１	ビットｂ０	意　味
0	0	オリジナルオブジェクト及びコピーをスクランブルされないで記憶できる。
0	1	オリジナルオブジェクト及びコピーをスクランブルされて記憶できる。
1	0	オリジナルオブジェクトをスクランブルされないで記憶できるがコピーは記憶できない。
1	1	オリジナルオブジェクトをスクランブルされて記憶できるがコピーは記憶できない。

表２：スクランブルされていないオーディオオブジェクト

ビットｂ１	ビットｂ０	意　味
0	０又は１	オリジナルオブジェクト及びコピーをスクランブルされないで記憶できる。
1	０又は１	オリジナルオブジェクトをスクランブルされないで記憶できるがコピーは記憶できない。

３ｄ）フレームスクランブルされたビット、１ビット

１つのフラグビットが、問題のフレームがスクランブルされているか否かを表わす。スクランブルされたオブジェクトの内部には、スクランブルされていないフレームが存在する可能性があり、従って、フレーム特定的スクランブリング表示を有することが有利である。

３ｅ）既知の又は暗号化されたキーを用いてスクランブルされたフレーム、１ビ

ット

１ａと同じ。フラグビット値１はクリアキーに対応し、値０は暗号化されたキーに対応する。

３ｆ）使用される条件付きアクセスシステム、３ビット

１ｂと同じ。３つのビットで、最大で８つの異なる条件つきアクセスシステムを識別することが可能である。

３ｇ）暗号化アルゴリズム、６ビット

１ｃと同じ。６つのビットで、最大で64の異なる暗号化アルゴリズムを識別することが可能である。

３ｈ）記憶情報、21ビット

このフィールドは、２つのサブフィールドに分割される。

＊　例えば下表にあるように、記憶媒体識別子、４ビット（残りのビット組合せはさらなる拡張のために予約される）。

b 3			b 0	媒体
0	0	0	0	一斉通信
0	0	0	1	テープ
0	0	1	0	CD
0	0	1	1	ハードディスク
0	1	0	0	例えばローカルエリアネットワーク内の遠隔記憶装置

＊　年を表わす最後の２つの数字（０～９、共に４ビットでコード化されている）、月を表わす順序数（４ビットでコードされた１～12）及びその月の中の日（５ビットでコードされた１～31）を含み、局所記憶装置の場合には記憶の日付に対応し、一斉通信又はネットワーク記憶装置の場合には現在の日付に対応する、日付、８＋４＋５ビット。

３ｉ）許可データ、261 ビット

これまでに提示されたビットの合計数は８で等分できず、或る種のバイト特定的データをバイト境界から始めることが有利であるため、このフィールドは、有

利には、全て１である５つのパディングビットで始まる。これらのビットの後には、サービスプロバイダ識別コード、プログラム識別コード及びプログラム分類といったような使用される条件付きアクセスシステムに応じた情報を含む可能性のある32バイト(256ビット）の許可データフィールドが続いている。

３ｊ）暗号化された又はされていないキー、168 ビット

このフィールドは、以下の通りの３つのサブフィールドに分割される：

＊　スクランブル解除するためにどれぐらい長く現在のキーが使用されることになるかを示す、キー（８ビット）を伴う残りのフレームの数、

＊　現在のキー（80ビット）及び、

＊　次のキー（80ビット）

２キー方式により、受信又は復元装置には、次の暗号化されたキーを解読する時間が与えられる。残りのフレームの計数がゼロに達した時点で、新しいキーは現在のキーとなり、次のキーは新しいキーとなる。キーの実際長は、使用されるスクランブリングシステム及びキーの暗号化方法により左右され、従ってここで言及されている80ビットは、最大長にすぎない。

３ｋ）初期化修正子、40ビット

１ｇと同じ。

３ｌ）オーディオフレーム構造のための規格、８ビット

本発明によると、記憶書式はいずれの特定のオーディオフレーム構造にも結びつけられていないことから、記憶されたフレームデータの中でフレームが遵守する規格を指示することが有利である。フレームは、例えば動画像専門家グループ（MPEG）の規格に従ってＩSO／IEC 11172-3 Layer II又はLayer IIIフレームであっても、或いは又DAB オーディオフレームであってもよい。８ビットで標準識別子をコード化する場合には、将来のフレーム規格のために十分なスペースが取っておかれる。

３ｍ）３ａ～３１についてのハッシュ合計（hash sum）、88ビット

３ａ～３ｌで上述したフィールドは、受信及び／又は再生（プレイバック）と

結びつけてできるかぎり迅速に読取られうるように、有利にはスクランブルされないで残される。ただし、これらのフィールドは、無許可の修正に対し幾分か保護されていなくてはならない。本発明によると、いわゆるハッシュアルゴリズムが既知の要領で使用され、このアルゴリズムは３ｍフィールド内の最初の８つのビットにより識別され、前記フィールドのビット内容に基づき或る80ビットの結果を計算するのに用いられる。フィールド３ａ～３１の中味をハッシュ合計と比較することにより、ハッシュ合計が計算されたのちにフィールドの中味が変わったか否かを検出することが可能である。無許可の装置はハッシュアルゴリズムを知らないことから、修正されたヘッダフィールド値に対応するようにハッシュ合計を変更することはできない。

３ｎ）記憶されたスクランブルされた又はされないオーディオフレーム、可変長

フレームの最初に、各バイト内にオーディオフレームの長さを表わす16ビット長のサブフィールドが存在する。フレームの長さは、符号化方法、圧縮レベル及び考えられる補助データ(DAB中のプログラム関連データ、PAD)によって左右される。フレームの最初に長さ情報が含まれていることは、高速巻戻し、高速前送り及びサーチといったようなオペレーションの一助となる。

次に、本発明により記憶されたデータグループに付加されたデータグループ特定的情報について見て行こう。本発明の観点から見ると、本発明ではスクランブリング及び保護方式はデータグループレベルで実行されることから、ファイル特定的情報（２ｉ～２１）をいかにして記憶するかは重要ではない。提示された記録の数、順序

及びサイズならびにビット値及びビット組合せの仕様は、例として提示されているにすぎず、本発明を制限することは意図されていない。

４ａ）データグループの番号付け、24ビット

特定のファイルに関係するデータグループが、連続的に番号付けされる。この意味で、データグループはブロック又はセグメントと呼ぶことができる。連続的な番号付けは、高速巻戻し、高速前送り及びサーチといったオペレーションにおいて特に有利である。

４ｂ）オリジナル／コピー、１ビット

３ｂと同じ。

４ｃ）記憶属性、２ビット

３ｃと同じ。

４ｄ）データグループスクランブルされたビット、１ビット

３ｄと同じ。

４ｅ）既知の又は暗号化されたキーでスクランブルされたデータグループ、１ビット

３ｅと同じ。

４ｆ）使用された条件付きアクセスシステム、３ビット

３ｆと同じ。

４ｇ）暗号化アルゴリズム、６ビット

３ｇと同じ。

４ｈ）記憶情報、21ビット

３ｈと同じ。

４ｉ）許可データ、261ビット

３ｉと同じ。

４ｊ）暗号化された又はされていないキー、168ビット

３ｊと同じ。

４ｋ）初期化修正子、40ビット

３ｋと同じ。

４ｌ）４ａ～４ｋについてのハッシュ合計、88ビット

３ｍと同じ。

４ｍ）記憶されたスクランブルされた又はされないデータグループ、可変長

３ｎと同じ。

次に、本発明による方式の実現の一部としてスマートカード内の実時間クロックを考えてみよう。システム内に実時間クロックを内含することには正当な理由がある。すなわち、こうして、受信した一斉通信オブジェクトの即刻の復元と、

一斉通信書式内に（不当に）記憶されたオブジェクトの後日の復元とを区別することが可能となるからである。前述した通り、デジタルオブジェクトを記憶する装置は、一斉通信書式内にオブジェクトを記憶できないものの記憶に関連しては記憶情報フィールド（以上の３ｈ／４ｈ）内のいくつかのビットをそれらが記憶媒体を表わすような形で変更することができるように、設計され構築されるべきである。しかしながら、問題のビットを変更せず単に一斉通信書式内にオブジェクトを記憶する「海賊」装置を構築することが可能である。しかし、海賊装置はハッシュ合計（上記３ｍ／４１）のための計算アルゴリズムを知らないため、フレーム又はデータグループのタイムスタンプを変更し対応する新しいハッシュ合計を計算することはできない。復元装置に対しては、復元を可能にする前に、一斉通信－書式オブジェクトのフレーム又はデータグループ内のタイムスタンプをそれ自体の実時間クロックと比較することが要求されることから、海賊装置により行なわれた録音録画は、タイムスタンプと実時間クロックの比較がバイパスされる類似の海賊装置を用いてしか復元され得ない。し

かしながら合法的に販売されている復元装置の全てが前記比較機能を含んでいる確率は高く、従って、この方式は少なくとも大幅に、合法的装置を所有するようなユーザに対する一斉通信書式内に記憶された海賊コピーの販売を防ぐことができる。

前記実時間クロックは、有利にはスマートカードの中に位置設定されるが、これは、こうしてスマートカード内のその他の情報の変更と同じ既知の要領でその無許可変更を防ぐことができるからである。さらに、後で記述する要領で新しいキーを中にロードするため許可されたディーラに対しユーザが自分のスマートカードを提示したとき、スマートカード内のクロックがいじられた場合には新しいキーがロードされることはない、ということが必要である。以上で提示した通り、１日の精度でタイムスタンプがなされた場合には、まず第１に実時間クロックはそれ以上の精度で読取り可能である必要はなく、第２に、一斉通信書式内に記憶されたオブジェクトをその１日の間自由に使用できる、ということになる。より厳密な時間制御が適用されるべきである場合には、タイムスタンプのためによ

り多くのビットがフレーム及びデータグループの中で確保されていなければならなくなる。

実時間クロックの連続オペレーションのためには、スマートカードには、有利にはスマートカードが受信機及び／又は再生装置に接続されている時にはつねに荷電され得る小型再充電式バッテリである電源が具備されていなければならない。バッテリの電圧が一定のしきい値より低く降下した時点で、実時間クロックは有利には、そのオペレーションが禁止される遮断状態にセットされ、これは、許可された店の許可されたディーラによってか又は安全な双方向通信リンクを通すことによってのみ再び作動状態となり得る。遮断状態の除去に必要とされる秘密情報は、有利には、カードがユーザに納

品された時点でスマートカードの固定記憶装置内に記憶される。スマートカード内の実時間クロックを新しい時刻にセットしなければならない場合、例えばシステムがその全てのオペレーションにおいて或る標準時間(例えばグリニッジ平均時間、GMT)を使用しない場合で、各時間帯を横断しているとき、許可されたディーラによる類似のオペレーションが必要となる。

デジタルオブジェクトを受信及び／又は復元する通常のユーザのための装置が、スマートカード内の実時間クロックにより示された時刻を読みとりそれをユーザに表示することはできるが、この装置が、許可されたディーラからの許可無くそれを変更することはできない。

図１～４を参照しながら、ここで、オブジェクト及び／又はその一斉通信に関係する権利を所有する当事者に対する支払いを可能にする本発明によるシステム内のさまざまな権利及び対応するキーの売却及び譲渡について記述する。一例として描かれている実施形態においては、当事者は、オブジェクトの出版者(PUB；内容プロバイダでもある）、一斉通信者（broadcaster）（BR；サービスプロバイダでもある）及びユーザ（Ｕ）である。図中丸で囲まれた数字は、本発明を制限する意味をもたないが、さまざまなステップの１つの考えられる相互順序を表わしている。

図１により記述されているケースにおいては、ユーザＵは出版者PUB の代理人

から、望まれるオブジェクトを含む記録CDを買う。出版者はデータがスクランブルされた形（Ｓ）となり、記録の各フレーム（上述の３ｊ及び４ｊ）内に内含されているスクランブル解除に必要なキーが暗号化されるような形で、記録を製造した。記録の価格は、製造及び輸送コストに対応し、記録の中味の使用権に対する料金を含んでいない。暗号化されたキーを解読するのに必要とさ

れるキーは許可（authorization)と呼ばれ、Ａ１とマーキングされている。該当する金額＄を支払うことにより、ユーザは許可を得る。

図１の事象は、その発生順で以下の通りである：

① 出版者PUB は、スクランブルされた形（Ｓ）で記録CDを製作し、それに暗号化されたキーを付加する。キーを解読するには、許可Ａ１が必要とされる。

② ユーザＵは出版者PUB に対し、記録CDの価格及び記録の中味の使用権料金＄の両方を支払う。

③ 出版者PUB は、ユーザのスマートカードSC内に記憶することによって、解読に必要とされる許可Ａ１をユーザＵに与える。

④ ユーザはスマートカードSC及び記録CDを再生装置（図示せず）の中に挿入し、この再生装置は次に許可Ａ１を用いてキーを解読し、ユーザにオブジェクトを復元しながら記憶されたオブジェクトをスクランブル解除（US）する。

許可Ａ１は、それがユーザＵに対して記憶されたオブジェクトを使用する資格のみを付与するのか又はそれをコピーする資格も与えるのかに応じて、異なるものであり異なる価格をもつことができる。許可は、特定の出版者の全ての製作品を網羅する出版者特定的なものであってよく、この場合、問題のオブジェクトに関係する識別情報が、許可に加えてスマートカードSC内に記憶されなくてはならない。ユーザが後で同じ出版者からもう１つの製品を購入する場合、スマートカード内に再び許可をロードする必要はないが、新しい製品の識別情報だけロードする必要がある。

図２で描写したケースでは、ユーザＵは、出版者PUB から、前記出版者により製作され一斉通信者BRによって伝送されたオブジェクトの使用権を取得する。考え方としては、出版者特定的許可Ａ１及

び或る一定額の金銭が、或る一定の支払い＄の代償としてユーザのスマートカードSC内にロードされる、ということである。出版者PUB は、１つのオブジェクトを一斉通信者BRに転送し、そのオブジェクトがすでにスクランブルされ（Ｓ）、そのスクランブリングキーが暗号化され、許可Ａ１を必要とするようにする。一斉通信者は、問題のオブジェクトを一斉通信し、このオブジェクトはその後受信され、許可Ａ１を用いてユーザＵの装置によりスクランブル解除（US）される。

図２の事象は、その発生順で、以下の通りである：

① ユーザＵは、出版者PUB に対して、出版者特定的ライセンスフィー＄を支払う。

② 出版者PUB は、ユーザのスマートカードSC内に記憶することによって、解読上必要とされる許可Ａ１をユーザＵに与える。同時に、スマートカードには、或る一定額の「電子マネー」＄＄＄がロードされる。

③ 出版者は、スクランブルされた（Ｓ）オブジェクトを一斉通信者BRに転送し、それに対して暗号化されたキーを付加する。これらのキーを解読するには、許可Ａ１が必要とされる。

④ 一斉通信者BRはオブジェクトを一斉通信する。

⑤ ユーザは、受信機及び再生装置（図示せず）の中にスマートカードSCを挿入し、受信機及び再生装置は次に許可Ａ１を用いてキーを解読し、ユーザに対しオブジェクトを復元しながら受信されたオブジェクトをスクランブル解除（US）する。同時に、スマートカードSC内の或る一定額の電子マネーに使用済みのマーキングが付される。

スマートカード内にロードされた電子マネーは、ユーザが一斉通信されたオブジェクトを受信しこれを使用につれてそれに比例して

使用済みとマーキングされる。使用済みとマーキングされる金額は、有利には、ユーザが受信されたオブジェクトを単に復元するだけかそれとも後に使用するためそれを記憶するかに応じて異なる。或る一定のオブジェクト及び異なる使用目的に対応する価格を識別するのに必要とされる識別情報は、オブジェクトと共に一斉通信される。

図３は、一斉通信者BRが出版者PUB からオブジェクトを購入しそれらを無料でユーザＵに配給するような状況を描いている。この状況は、その他の点では図２の場合と同じであるが、支払いは出版者PUB と一斉通信者BRの間で行なわれ、一斉通信者BRは、解読に必要とされる許可Ａ１を得る。一斉通信者はオブジェクトをスクランブル解除（US）しそれを、受信装置が一斉通信から直接読取ることのできる暗号化されていないキーで完全にスクランブルされないで又はスクランブルされて一斉通信する（上記３ｅ及び４ｅ参照）。このときユーザのスマートカード内では、いかなるマネーも使用済みとマーキングされず、実際、ユーザは自ら支払わなくてはならない許可に対する必要性が全く無くなる。

スマートカードと結びつけた電子マネーの概念は、そのままの形で既知のものである。スマートカードは、その中にロードされた或る一定額のマネーを誰にでもどんな料金でも支払うために使用することができるということを意味する「共通マネー」、又は或る一定の目的のためにマーキングされたマネーのいずれでも含むことができる。本発明によるシステムにおいては、このことは特に、どの出版者からのオブジェクトに対する支払いについても共通のマネーを使用することができる一方で、或る一定の目的すなわち単一の出版者のためにマーキングされたマネーはその特定の出版者から来たオブジェクトについての支払いのためにしか使用できない、というこ

とを意味している。後者の方式は、出版者が許可のローディングと結びつけてすでにお金を得、しかも何が誰にどのサービスの代償として支払われたかに関する混同が全くなくなることから、より優れたものである。

図２について上述された本発明の実施形態は、ユーザが出版者特定的許可Ａ１を獲得しなかった場合、このユーザは、一斉通信者BRによりスクランブルされて一斉通信されたその特定の出版者PUB からのいかなるオブジェクトも使用することができない、という欠点をもつ。この欠点は、ユーザＵが一斉通信者特定的許可A2の代償として＄を支払い、自分のスマートカード内にその一斉通信者BRに対しマーキングされた電子マネーをロードする、図４による変形実施形態により除去できる。出版者PUB は、オブジェクトがスクランブルされ（Ｓ）、そのスクラ

ンブリングキーが暗号化され許可Ａ１を必要とするように、一斉通信者BRに対し、１つのオブジェクトを転送する。一斉通信者BRは、キーを解読し、オブジェクトをスクランブル解除（US）するが、次に、新しいスクランブリングキーが暗号化され許可Ａ２を必要とするように再びオブジェクトをスクランブル（Ｓ）する。一斉通信者はその後許可Ａ２を用いてユーザＵの装置により受信されスクランブル解除（US）されるようなオブジェクトを一斉通信する。

一斉通信者BRと出版者PUB の間の合意により、ユーザが出版者のオブジェクトをどれほど使用したかに応じて出版者が支払いを受けることが要求されている場合には、ユーザのスマートカードSCは、一斉通信者特定的な金額を出版者の勘定に分割し、オブジェクトの使用（直接的使用、記憶、コピー）に従って勘定に借方記入する。後に、ユーザは、自分のスマートカードを一斉通信者、出版者又は許可されたディーラにより読みとらせ、ここで勘定が読取られ、こ

のとき一斉通信者は出版者に対し対応する金額を支払わなくてはならない。スマートカードは又、安全な双方向通信リンクを通してユーザの自宅で読取ることもできる。ユーザが自分のカードを読取らせるよう動機づけするため、スマートカード内のそれぞれの勘定が清算される前にユーザが記憶されたオブジェクトを後で使用できないような形で、許可を整備することが可能である。

図４中の事象は、その発生順で、以下の通りである：

① 出版者PUB 及び一斉通信者BRは、一斉通信に合意し、出版者PUB は一斉通信者BRに対し、解読のために必要とされる許可Ａ１を与える。

② ユーザＵは、一斉通信者BRに対し、一斉通信者特定的ライセンスフィー＄を支払う。

③ 一斉通信者はユーザＵに対し、ユーザのスマートカードSC内に記憶することによって解読に必要とされる許可Ａ２を与える。同時に、或る一定額の「電子マネー」がスマートカード内にロードされる。

④ 出版者PUB は、スクランブルされた形（Ｓ）でオブジェクトを一斉通信者に送り出し、それに暗号化されたキーを付加する。キーを解読するためには許可Ａ１が必要とされる。

⑤　一斉通信者BRは、スクランブリングキーを解読するために許可Ａ１を用い、受信されたオブジェクトをスクランブル解除（US）するが、次に解読に許可Ａ２が必要となるような形でそれを再びスクランブル（Ｓ）する。次に、一斉通信者はこのオブジェクトを一斉通信する。

⑥　ユーザはスマートカードSCを受信機及び再生装置（図示せず）内に挿入し、この受信機及び再生装置は、許可Ａ２を用いてスクランブリングキーを解読し、ユーザに対しオブジェクトを復元する一

方で、受信されたオブジェクトをスクランブル解除（US）する。同時に、スマートカードSC内の或る一定額の電子マネーに使用済みのマーキングが付される。

⑦　出版者と一斉通信者の間の合意により必要とされる場合、ユーザは自らのスマートカードSCを読ませ、一斉通信者BRは、スマートカード内のデータに基づいて出版者PUB にライセンスフィーを支払う。

ユーザのスマートカード内にロードされた上述のすべての許可は、固定した時間中、又はさらなる通知があるまで有効であり得る。スマートカード内の実時間クロックは、固定期間機能（fixed-period feature）の実現において有用である。というのもこのとき受信機及び再生装置はクロックをもつ必要がなくなるからである。また、或る１つの装置内のクロックの場合よりもスマートカード内のクロックの場合の方が、いたずらするのが困難である。

１つのオブジェクトの受信及び使用がスマートカード内に記録された場合、自分のスマートカードを許可されたディーラに提示することによりユーザは自分がすでにそのオブジェクトの使用に対し支払いを済ませていることを示すことができ、図１にあるように少額の追加料金でオリジナルの記録を得ることができるように配慮することができる。

本発明では、一斉通信でのデジタルオブジェクトのスクランブリングが先行技術で知られているため、既知のオブジェクト一斉通信メディアには全く変更を必要としない。本発明による端末装置は、既知の方法を用いてスクランブルされた伝送を受信しスクランブル解除するため、及びメモリ媒体上に記憶された許可を用いてスクランブリングキーを解読するための手段を内含していなくてはならな

い。さらに、記憶用端末機器には、記憶段階において上述の記憶書

式を生成し、再生段階でそれを読みとるための手段が内含されていなくてはならない。これらの手段は、端末機器又はその制御下で作動するその他のプログラミング可能な装置のオペレーションを制御するマイクロプロセッサにより実行されるソフトウェアプロセスとして有利に実施され、かかるプロセスは、当業者により日常的に作成されるものである。

【図１】

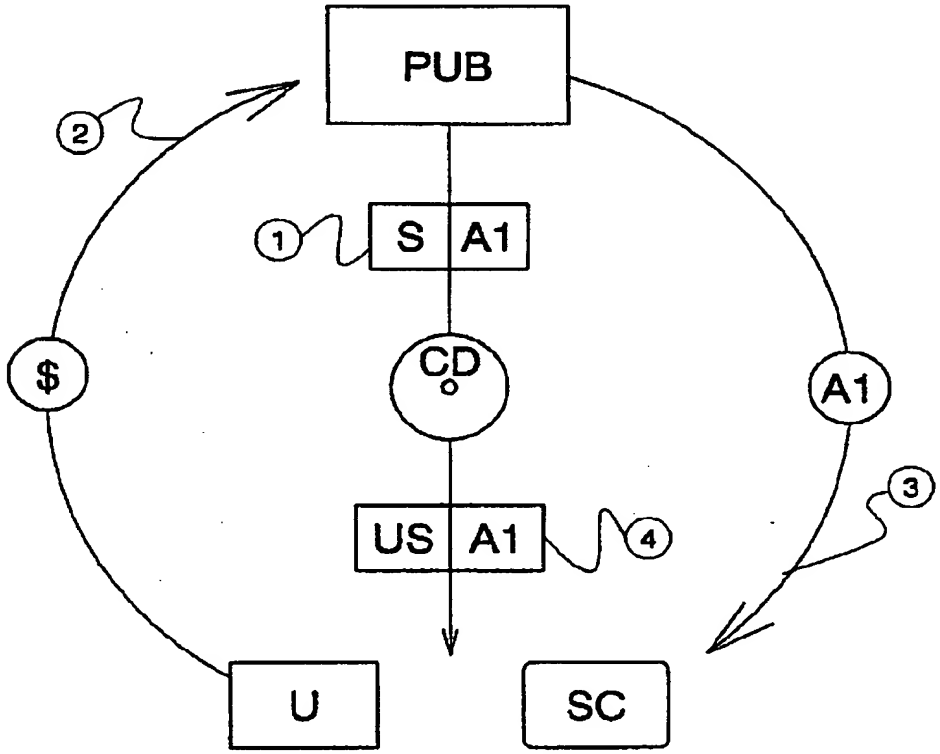


Fig. 1

【図２】

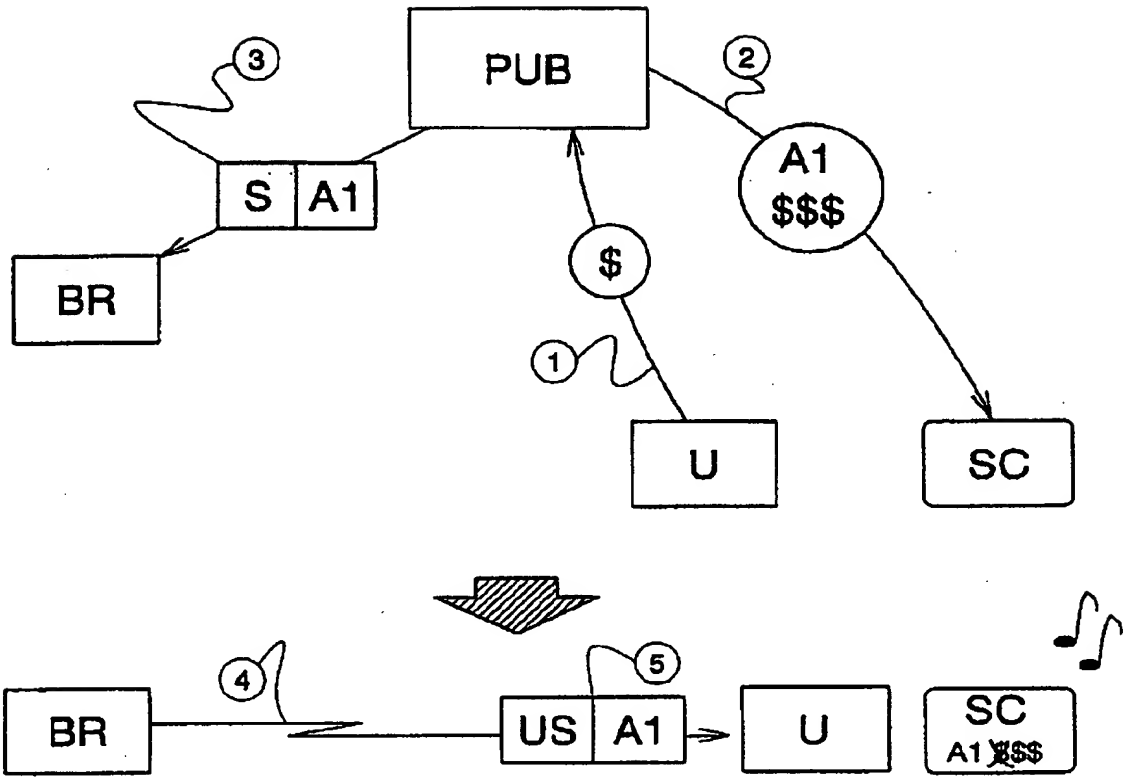


Fig. 2

【図３】

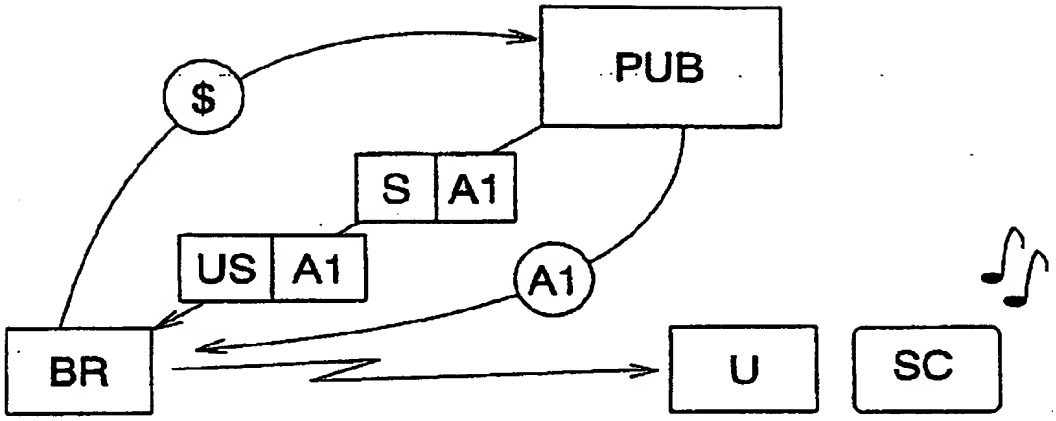


Fig. 3

【図４】

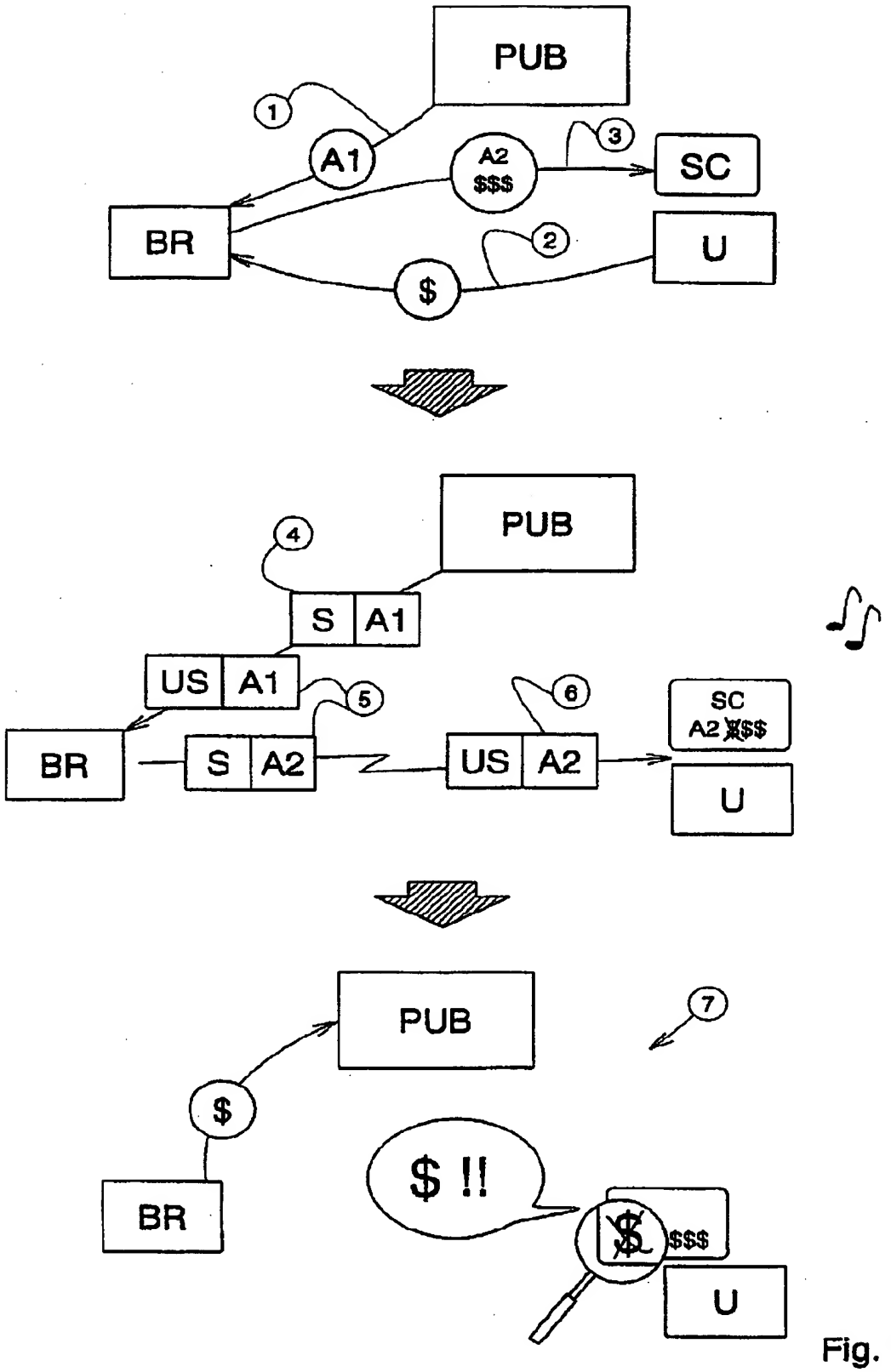


Fig. 4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 97/00045

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04N 7/167
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	EP 0710025 A1 (SONY CORPORATION), 1 May 1996 (01.05.96), abstract --	1-11
A	EP 0666694 A1 (GENERAL INSTRUMENT CORPORATION OF DELAWARE), 9 August 1995 (09.08.95), abstract --	1-11
A	WO 9113517 A1 (KUDELSKI S.A. FABRIQUE D'ENREGISTREURS NAGRA), 5 Sept 1991 (05.09.91), abstract --	1-11
A	EP 0674440 A2 (NOKIA TECHNOLOGY), 27 Sept 1995 (27.09.95), abstract --	1-11

☐ Further documents are listed in the continuation of Box C.　　☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"B" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 April 1997	08 -05- 1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

02/04/97

International application No.
PCT/FI 97/00045

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0710025 A1	01/05/96	JP 8181689 A	12/07/96
EP 0666694 A1	09/08/95	AU 676404 B	06/03/97
		AU 8150894 A	10/08/95
		CA 2137616 A	03/08/95
		JP 8107412 A	23/04/96
		NO 944678 A	03/08/95
		US 5504816 A	02/04/96
WO 9113517 A1	05/09/91	AT 147918 T	15/02/97
		AU 647080 B	17/03/94
		AU 7210691 A	18/09/91
		CA 2051810 A	22/08/91
		CH 682614 A	15/10/93
		DE 69124159 D	00/00/00
		EP 0469106 A,B	05/02/92
		HU 62131 A	29/03/93
		IL 97189 A	19/01/96
		JP 4505538 T	24/09/92
		US 5375168 A	20/12/94
EP 0674440 A2	27/09/95	FI 95756 B,C	30/11/95
		FI 941316 A	22/09/95

フロントページの続き

(81)指定国　　EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN